to the transmission of messages over a portion of the period and also related to the position of the portion in the period, to enable output data to be derived from the stored information;

(ii) creating a second signature comprising a plurality of parameters related to the transmission of messages over a second period shorter than the first and more recent than the first;

(iii) updating the first signature by a weighted averaging with the second signature; and

(iv) deriving said anomalies by providing said signatures as input to an anomaly detector.

2. (once amended) A method as claimed in claim 1 wherein the first signature is created in one of a plurality of predetermined possible formats.

3. (once amended) A method as claimed in Claim 2 wherein the format of the first signature comprises the length of the signature.

4. (once amended) A method as claimed in Claim 1 wherein said at least one parameter represents the number of events made in the portion of the first time period as a proportion of the total number of events made in the whole first time period.

5. (once amended) A method as claimed in Claim 1 wherein said at least one parameter represents the number of events of a predetermined type made in the whole first time period as a proportion of the total number of events of the same type made in the whole first time period.

6. (once amended) A method as claimed in Claim 1 wherein the step of creating a signature further comprises the steps of:

storing information about each of a number of events which occurred during the first time period;

selecting attributes from this information;

and converting the attributes into the said first signature.

Cancel claim 7 without prejudice.

Amend claim 8 as follows:

8. (once amended) A method as claimed in Claim [7] 1 wherein [the anomaly detector comprises] said step (iv) of deriving anomalies comprises providing said signatures as input to a neural network.

Cancel claim 9 without prejudice.

Amend claims 10 through 13, 18 and 21 and 22 as follows:

10. (once amended) The method of Claim 1 wherein [the data deriving] said step (iv) of deriving anomalies is carried out using a predictive model, the method further comprising the steps of:

monitoring the performance of the model; and

automatically updating the model when the performance reaches a predetermined threshold.

11. (once amended) The method of Claim 1 wherein [the data deriving] said step (iv) of deriving anomalies is carried out using a predictive model, and wherein the model is implemented using at least one instantiated object created using an object oriented programming language and the method further comprises the steps of:

converting the object into a data structure;

storing the data structure; and

recreating the object from the data structure.

12. (once amended) A computer system for detecting anomalies in the transmission of messages by an entity by storing information relating to the transmission of messages by [an] the entity over a given time period, said computer system comprising:

(i) an input arranged to receive information about each of a number of events which occurred during the time period;

(ii) a processor arranged to convert the information into a signature comprising a plurality of parameters related to the transmission of messages over the time period wherein the parameters comprise at least one parameter related to the transmission of messages over a portion of the period and also related to the position of the portion in the period, to enable output data to be derived from the stored information and wherein said processor is further arranged to convert at least part of the information into a second signature, comprising a plurality of parameters related to the transmission of messages over a second period, shorter than the first and more recent than the first; and also to update the first signature by a weighted averaging with the second signature; and

(iii) an input arranged to provide said signatures to an anomaly detector to derive said anomalies.

13. (once amended) A method of deriving [output data] anomalies from information relating to the transmission of messages by an entity over time, comprising the steps of:

(i) creating a first signature comprising a plurality of parameters related to the transmission of messages over a predetermined first time period;

(ii) creating a second signature comprising a plurality of parameters related to the transmission of messages over a second period shorter than the first and more recent than the first;

(iii) updating the first signature by a weighted averaging with the second signature;

and (iv) deriving said anomalies using the signatures.

18. (once amended) A method as claimed in Claim 13 wherein [the deriving step comprises the step of detecting anomalies in] said information relates to the transmission of messages in a telecommunications network.

21. (once amended) The method of Claim 13 wherein [the data deriving] said step ~~(iv) of~~ deriving said anomalies is carried out using a predictive model, ~~and~~ wherein the model is implemented using at least one instantiated object ~~created~~ using an object oriented programming language and the method ~~further~~ comprises the steps of;

converting the ~~object~~ into a data structure;

storing the data structure; and

recreating the object from the data structure.

22. (once amended) A computer system for deriving [output data] anomalies from information relating to the transmission of messages by an entity over time, the system comprising:

an input arranged to receive information about the transmission ~~of~~ messages by the entity;

a processor arranged to create a first signature comprising a plurality of parameters related to the transmission of messages over a predetermined first time period and to create a second signature comprising a plurality of parameters related to the transmission of messages over a second period shorter than the first ~~and~~ more recent than the first;

a processor arranged to calculate a weighted averaging of the first and second signatures to form an updated first signature;

and a processor arranged to derive said [output data] anomalies using said signatures.